Statewide IT Policy Title: **Information Technology Security Policy**

Effective Date: June 26, 2002 Policy Number: P-104

Table of Contents

I.

A. Policy Statement

It is the policy of the State of Colorado to secure and protect the State's information technology resources and information assets as a critical business priority**.** Also, it is the policy of the State that each agency develop and implement an information security program and utilize a layered security approach to protect its IT assets. This agency-internal information security program and policy shall consist of these eight [8] components:

1. Business impact analysis that assesses the criticality of services
2. Risk/security assessment that identifies environment vulnerabilities
3. Risk management process
4. Contingency plan for disaster recovery/business continuity
5. Identifies Security safeguards for asset protection
6. Secure architecture design
7. Developed security awareness and training programs
8. Monitor/audit system for back end reviews and efficiency/effectiveness analysis.

Further, it is the policy of the State to designate an individual to act as a State Chief Security Information Officer and for each agency to designate an individual to coordinate its security policy, needs and requirements with this Office.

B. Statutory Authority

C.R.S. 24-37.5-104(1); C.R.S. 24-37.5-106(1)(c); C.R.S. 24-37.5-203(1)(a); C.R.S. 24-37.5-204; C.R.S. 24-71.1-101, C.R.S. 24-71.1-109, C.R.S. 24-71.1-110(1)(a); C.R.S. 24-37.5-202(1)

C. Coordinating Agency Authority

C.R.S. 24-37.5-204; C.R.S. 24-71.1-106, C.R.S. 24-71.1-109, C.R.S. 24-30-901, et seq., C.R.S. 24-30-1603

II. Purpose

The purpose of this policy is to recognize that security is a mission critical business requirement for all government operations, that the State's communications and information resources are valuable strategic assets that belong to the people of Colorado and that they must be managed accordingly. In addition, the policy's purpose is to assist agencies in protecting those privacy rights established under the law associated with certain information as provided by law and identify the best practices used to maintain the integrity and reliability of information. Moreover, it identifies those elements of the network and IT environment that must be protected to meet the goals and of the policy and provides direction for leveraging scarce resources to best protect the State's IT investment. Further, by identifying the necessary elements of an effective risk analysis and risk management framework, it assists the State in achieving and maintaining a more efficient, effective, stable statewide IT environment.

The primary objectives of this policy are:

- To effectively manage the risk of security exposure or compromise within and among systems;
- To establish the responsibilities for the protection of information as well as to establish a secure IT base and a stable IT environment;
- To promote a coordinated understanding of the State's security needs and compliance with security requirements in accordance with all applicable laws and regulations;
- To provide management flexibility in the event of an information asset misuse, loss or unauthorized disclosure;

III. Scope

This policy applies to all State agencies as defined in CRS 24-37.5-102(5).

IV. Exemptions

Agencies are discouraged from filing a request for exemption from this policy. OIT and OSPB may jointly approve exemptions on a case-by-case basis if the request is supported by extraordinary circumstances. All requests for exemption will be handled as set forth under the procedures of the General Exemption policy.

V. Related Policies, Standards, Guidelines

A. Core Policies

1. Privacy – The required environment must be secure before privacy can be effective; privacy is thus assured.
2. Interoperability – While security risk can be reduced through a refocus and recommitment of budgetary resources, risk can also be increased due to the integration of previously separate target sites.
3. Infrastructure – A secure environment is created through infrastructure while security determines the method of delivery that shapes infrastructure
4. Life Cycle Management – Maintained security must be done through life cycle management as the dynamic nature of security enables the lifecycle to be constantly evaluating and updating security practices. Security can adversely affect life cycle management due to unforeseen events of component vulnerability.
5. Project Management – Security is achieved through effective project management.
6. Aggregation – As with interoperability, security risk can be either reduced or increased through aggregation. Conversely, security can limit/impact aggregation.

B. Related Policies

The following policies have been prioritized, presented in sequential order, based upon their resource impact (most to least), capability for implementation within fiscal restraints and statewide, common elements.

1. Data Classification System*
2. Access Control*
3. Server Backup*
4. Contingency Planning Disaster Recovery – 7/30/90
   a. See http://www.oit.state.co.us/commissions/imc_doc_strat_cpdr.asp

* Publication date for these policies TBD

C. Related Standards

D. Related Guidelines

Publication date for the Guidelines for the eight [8] components listed in the Policy Statement is TBD. Agencies may determine the specific risk analysis and management tool to be utilized for developing its strategy and framework.

See Appendix A for the Recommendations

VI. Impact

State Agencies shall incorporate these policy components into their business strategies and annual budget review process. All IT investments initiated or implemented after July 1, 2002 must be developed in compliance with this policy. State Agencies shall provide satisfactory evidence of compliance with this policy upon the request of OIT or OSPB**.** The OIT will deny all procurement requests that do not comply with this policy.

A. Implementation

Each State Agency shall immediately construct and implement a security program. As part of that program, in prioritized order, agencies shall develop security polices that address, at a minimum, the following:

1. Virus Protection/Detection
2. Firewall Security
3. Logging Capability
4. Server Security
5. Intrusion Detection
6. Encryption
7. Physical Security
8. Secure Remote Access Communications (if applicable)

OIT understands that compliance with this policy is constrained by the present budget situation. However, agencies are expected to develop a migration plan that sets out the Agency's goals and objectives and establishes priorities for reaching full compliance within the next five years. Moreover, these criteria set out in this policy are a baseline. Security, as a critical State concern, must be incorporated and addressed in each budget request/project plan and subsequent Request for Proposal [RFP] along with a developed business case for said requests/projects. Future IT project requests shall include costs for necessary and appropriate security components to be consistent with the Agency's ongoing security plan and policy. All future IT requests will be denied if not in compliance with respect to the requirements of this policy.

OIT shall name a State Chief Information Security Officer [ISO]. It shall serve as the facilitating coordinator between DPS and State agencies.

B. Compliance

The Executive Director or agency head is responsible for the security of that agency's information technology resources. As such, each Agency shall develop, document and implement a security program consistent with the eight [8] components outlined in the Policy Statement and security policies that evidence compliance with the eleven [11] requirements set out above. In addition, agencies shall develop a migration plan that establishes its timeline toward achieving the eight [8] components outlined in the Policy statement. Agencies shall coordinate with the Division of Information Technology [DoIT] within the Department of Personnel and Administration [DPA] for operational purposes and the Department of Public Safety [DPS] for physical security purposes in developing and implementing its program. Failure to comply with this policy may result in that specific agency being removed from and denied access to the State network or mainframe [OCIN and/or CIN] until such compliance is demonstrated.

VII. Maintenance

Technological advances and changes in the business requirements of agencies will necessitate periodic revisions to this policy. Policy will be reviewed and updated as appropriate and/or at least annually.

VIII. Effective Date

This policy shall be effective from date of approval from the Chief Technology Officer of Colorado.

Marc Holtzman